June 1, 1977

Subcommittee Report to the SCC
Executive Summary

Re: Unauthorized Disclosure of Sensitive Information

The attached report to the SCC is made pursuant to PRM/NSC-11 by the subcommittee acting under the direction of the Attorney General.

The report addresses the problem of unauthorized disclosure of classified information. Because this problem relates directly to the classification system itself, the report concludes that a thorough review of that system is a necessary first step to any resolution of the problem of leaks. In addition, the report notes that the existing criminal laws barring the unauthorized disclosure of certain specific kinds of classified information have not been enforced over several Administrations because of the various political and security costs involved in investigating and prosecuting leaks.

The subcommittee concludes that the same policy reasons which have precluded the investigation and prosecution of leaks in the past are still relevant and that the price for passage of legislation generally criminalizing the unauthorized disclosure of classified information is a price too high to pay for the marginal utility of such legislation.*/

Other means of addressing the problem of unauthorized disclosures are also discussed, e.g., reducing access, Secrecy Agreements, disciplinary measures, civil actions, increased use of polygraphs, and the conclusion is that no feasible option is likely to have more than the most marginal impact on leaks, while each option has significant negative costs.**/

---

*/ The CIA dissents from this conclusion. Its conclusion and the reasons therefor are attached as Appendix 1.

**/ The Department of Defense takes exception to the thrust of the subcommittee's report on Secrecy Agreements and in addition wishes to emphasize the importance of investigating leaks even if prosecution is not the desired end. The Department of Defense's views are attached as Appendix 2.

May 31, 1977

REPORT TO THE SCC PURSUANT TO PRM/NSC-11

Re: Unauthorized Disclosure of Sensitive Information

Leaks of sensitive information have plagued the Government for a number of years, and in recent years as a result of a growing distrust of the Executive and investigations of intelligence agencies such leaks have been relatively more numerous.*/ There has been a consistent sense of frustration on the part of the Executive at the apparent inability to take effective action against leaks.

The information leaked in just the past several years has included military secrets, foreign policy secrets, and intelligence secrets--the latter two being the most sensational. Ordinarily such information is classified pursuant to E. O. 11652, which requires a determination at the minimum that information to be classified, if disclosed without authorization, "could reasonably be expected to cause damage to the national security." This is the basic Executive-wide standard for determining which information is to be protected against

---

*/"Leaks," for purposes of this report, refer both to anonymous leaks to the press and to attributed publications by persons who previously had access to classified information.

unauthorized disclosure, and the application of certain criminal statutes turn on whether information is so classified. See 18 U.S.C. § 798, 50 U.S.C. § 783(b) & (c). As such, the Order as written and the practice under it cannot be separated from the problem of leaks.

E.O. 11652 was issued in 1972 in an attempt to correct the problems perceived in E.O. 10501, as amended, which had been the basis for the classification system. The perceived problems included rampant overclassification, the lack of an effective downgrading and declassification process, and too widespread authority to classify information. E.O. 11652, therefore, significantly restricted the number of persons who could originally classify information Secret or Top Secret, created schedules for review and declassification of information exempted from automatic downgrading and declassification, prohibited overclassification and unnecessary classification, prohibited classification to conceal inefficiency, administrative error, or to prevent embarrassment to a person or department, and created the Interagency Classification Review Committee (ICRC) to "review and take action to ensure compliance" with the Order. Nevertheless, the same problems remain today as before E.O. 11652, with little significant

change. That is, while the number of persons with original classification authority for Top Secret and Secret has been cut, although the number is still large, any employee may by "derivative authority" classify documents.*/ The exemptions from the General Declassification Schedule are overused, and information so exempt need only be reviewed after 10 years, and then only upon a request for review. And finally, the prohibition against over-classification has simply been ineffective, and it may be fairly said that the greatest abuses have been at the highest levels of Government, either through outright overclassification or because information overclassified at lower levels is not, when it comes to the attention of higher authorities, promptly sent back for downgrading or declassification.

The result of these continuing problems is a cynical attitude toward classified information by many in the Executive Branch, Congress, and the public. This cynical attitude is reinforced when classified information is deliberately disclosed by responsible officials, yet the

---

*/ If information is extracted from a classified document, it must be "derivatively" classified. For example, PRM/NSC-11 is classified Secret, but because it does not indicate what information therein is and is not classified, even the letters and numbers "PRM/NSC-11," should be classified Secret whenever referred to in another document. This obviously leads to unnecessary classification.

information remains classified, e.g., PD/NSC-2 was classified Confidential, but its entire substance was briefed to the press by the White House Press Office immediately upon its issuance.*/ While it is difficult to assess the extent to which this cynical attitude is responsible for leaks, there are certain leaks which may be fairly confidently attributed to this attitude, e.g., many of the leaks originating from the House Intelligence Committee. Perhaps more important, the cynical attitude toward classified information in Congress, where repeated statements assert that 99% of classified information need not be classified, makes any new statute either rationalizing the existing criminal penalties in the manner of S. 1 or extending prohibitions, as President Ford's suggested bill would have done, most difficult, if not impossible, to pass.

The subcommittee recommends that a thorough review of E.O. 11652 be made for the purpose of again attempting

---

*/ The widespread and blatant disregard for various provisions of the Executive Order, e.g., Section 4(A), condoned by the silence of high authorities, if not evidenced by them, further engenders a disrespect for the Executive Order generally and raises questions about attempts to maintain a strict standard as to other provisions, i.e., prohibitions against unauthorized disclosure.

to de[illegible] safeguards against overclassification, but the subcommittee recognizes that no systemic changes, absent Draconian measures, can ever substantially alleviate the problem of overclassification absent a strong and continuous commitment by those high in Government to scrutinize closely everything they classify and everything which comes to their attention under their delegations to insure that information is not classified or exempted from general downgrading and declassification unless the information clearly warrants it.

The subcommittee also suggests that substantial consideration be given to placing the oversight role, as the ICRC and the NSC have under E.O. 11652, in an independent body such as the IOB, which would not reflect the institutional biases that inevitably result when the proverbial foxes are guarding the hen house.

Notwithstanding the limitations of E.O. 11652, it cannot be doubted that the majority of leaks would have occurred whether or not the classification system itself was perfect. And there is general agreement that the Executive Branch's actions to combat leaks has been ineffectual. Indeed, in the majority of cases no action

at all has been taken, either preventive or investigative.*/ In many cases the lack of action was a deliberate decision by those involved; in some the lack of action occurred for lack of a decision.

To understand the reasons why a conscious decision not to investigate was made, and to assess the validity of such decisions, it is necessary to describe the limitations of current law, self-imposed Executive Branch limitations, and the costs of investigating and taking action against leakers.

It has often been pointed out that there exists no law which generally prohibits the unauthorized disclosure of classified information. The statutes which specifically refer to classified information, 18 U.S.C. § 798 and 50 U.S.C. § 783, respectively prohibit the unauthorized disclosure of classified communications intelligence information and the unauthorized communication of classified information to an agent of a foreign government or a

---

*/ For purposes of the Report the formation of the "Plumbers" Group and its activities, wrongheaded in its conception and largely illegal in execution, are considered the equivalent of "no action," because it was the perceived inability to take other effective action which led to the formation of the "Plumbers."

member of a Communist organization. */ The Espionage Act, 18 U.S.C. § 793(d) & (e), prohibits the communication of "information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation" to a person not authorized to receive it. While the term "national defense" has been broadly construed to mean "a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness," Gorin v. United States, 312 U.S. 19, 28 (1941), it is doubtful whether the term even so construed includes all foreign relations matters and intelligence matters. For instance, it would be difficult to characterize the information in the Washington Post article dealing with payments to King Hussein as information relating to the national defense. Thus, many leaks have occurred which do not seem to fall within the proscription of any criminal statute. **/

---

*/ 42 U.S.C. § 2277 carries a $2,500 criminal fine for the unauthorized disclosure of atomic energy information which is "classified" pursuant to the statutory classification system for such information, see 42 U.S.C. § 2161 et seq.

**/ The current bill to revise the criminal code will not affect any of these statutes.

Even where a leak might be covered by a criminal statute, prosecution may be inadvisable. First, all of the above statutes require at the minimum that the information disclosed be entered into evidence*/ and that the prosecution prove either that it was classified or that it was in fact national defense information. To do this requires declassification of the information and confirms the accuracy of the information disclosed.**/ In addition, in prosecutions under 18 U.S.C. § 793(d) or (e), it is necessary for the Government to prove that the leaker could reasonably believe that the information could harm the United States or aid a foreign nation. On the one hand, this can be exceptionally difficult to prove, especially where no apparent harm or aid has resulted from the leak (this was the case in the Ellsberg trial). Effective proof on this point may require further

*/ This much is probably constitionally required.

**/ Because at one time the FBI routinely investigated leaks only to be informed after the expenditure of manpower and resources that the affected agency would not declassify the necessary information for prosecution, the FBI has now for several years required agencies requesting investigations of leaks to complete a form which in effect amounts to an agreement to declassify the necessary information for prosecution. Between 1965 and 1973 at least fourteen suspected leaks were not investigated or prosecuted because the affected agency would not declassify the necessary information.

disclo[illegible] of classified information--[illegible]ther the harm or aid which has resulted or other classified information to demonstrate how in context the information disclosed could harm the United States or aid a foreign nation.

Because of the inadequate coverage of existing laws and the difficulties involved in prosecutions under them, the Executive Branch has attempted without success since at least 1957 to obtain new legislation which would generally criminalize the unauthorized disclosure of classified information. A law providing criminal penalties for the unauthorized disclosure of classified information by a Government employee would close a loophole that exists in the law less through conscious decision than through inadvertence. It would be consistent with other laws which punish the unauthorized disclosure of information by Government employees, see 5 U.S.C. § 552a(i)(1) (information disclosed in violation of the Privacy Act); 18 U.S.C. § 1902 (disclosure of crop information); 18 U.S.C. § 1905 (disclosure of trade secrets or financial information required to be reported to the Government); 18 U.S.C. § 1906 (disclosure of names of borrowers or collateral for loans by a bank examiner).

The subcommittee, however, has concluded that the costs of passage of such legislation if it could be passed at all, probably outweigh the marginal utility such legislation would have, at least at the present time. The subcommittee is of the view that until the Executive Branch has effectively utilized the laws and mechanisms now available to it to prevent and investigate leaks, no new legislation should be sought.

This conclusion is based on the fact that in the past even where an effective statute was available, e.g., 18 U.S.C. § 798, no investigative or prosecutorial action has been taken. The reasons for this lack of action are likely to continue even if a law generally prohibiting the unauthorized disclosure of classified information were enacted.

There are several reasons why the Executive has failed to take action on leaks in the past. First, an investigation may give added publicity to the leaked information or confirm its accuracy, thereby compounding the problem. Second, as the Daniel Ellsberg case illustrates, prosecutions against leakers may have an adverse, rebound effect because of a perception that the Government is

trying to cover-up wrongdoing or impropriety. This perception is reinforced if the leak involves allegations of misconduct or wrongdoing. Third, leaks are often traced to Congressional committees; investigations of members of Congress or their staffs carry high political costs. Fourth, leaks are often made to newsmen who are either protected from forced disclosure of their sources or are prepared to stand in contempt rather than do so. Fifth, the Department of Justice has consistently refused to undertake criminal investigations unless the affected agency agrees to declassify by time of trial the information necessary to obtain a conviction, and intelligence agencies have generally refused to make such an agreement. Sixth, in some cases the affected intelligence agency has acted unilaterally or in concert with the intelligence service of another government in such a way as to taint any possible case against the individual. Seventh, there has been a wide-spread notion that leaks would gradually dry up as investigations of, and the consequent interest in, intelligence agencies' activities came to an end. Eighth, there has been some skepticism whether investigative efforts within lawful boundaries would be able to determine the source of leaks, the concern being that an unproductive investigation would demonstrate the Government's impotence.

Because these considerations cut across institutional lines, in the past neither the White House, the affected intelligence agencies, nor the Department of Justice has been willing to push for investigation. Therefore, unless and until all affected agencies jointly decide that the price for investigation and vigorous prosecution is a price worth paying to counter leaks, no additional legislation will have more than the most marginal effectiveness. Moreover, as the Executive has demonstrated that it is unwilling to investigate and prosecute leaks under a criminal statute already on the books, 18 U.S.C. § 798, there is little basis for the Executive to request legislation prohibiting leaks of classified information in other areas.

It has been suggested that civil penalties could be utilized to punish leaks. Civil penalties could be of two sorts--(1) civil fines or (2) disciplinary action against current Executive Branch officers and employees. The first would require legislation. In addition, where the leaker was unknown many of the factors weighing against investigation would remain, and some of the tools available to investigate criminal offenses--e.g., the grand jury--would

be unav[illegible]ary to introduce into evidence the classified material leaked, thereby confirming the accuracy of the leak. Moreover, it would be difficult to determine the scale of a civil fine that would provide an adequate deterrence to those who stand to make substantial sums by publishing their memoirs. Finally, it would present an anomaly for disclosure of crop information to carry a criminal penalty, see 18 U.S.C. § 1902, but disclosure of national security secrets to carry a civil penalty.

The second option--disciplinary action against employees--would not require new legislation. Such disciplinary action could range from removal of a security clearance to suspension and discharge of the employee, see 5 U.S.C. § 7532. While in most cases the employee would be entitled to a hearing prior to discharge, it might be possible to avoid disclosure of classified information in the hearing consistent with the employee's due process and statutory rights.*/ This possibility alone makes this an attractive option.

This option could, of course, only be utilized against current members of the Executive Branch, and thus is limited.

---

*/ Prior to or concurrent with an initiation of a program to investigate and take disciplinary measures against employees, a full review and probable rewriting of regulations regarding such disciplinary actions will be required to assure that they comport with statutory and constitutional requirements.

Moreover, investigations to determine the identity of a leaker will again be frustrated by the inability to compel cooperation or testimony. The FBI is of the view that in the overwhelming majority of cases the leaker will not be able to be found pursuant to such an investigation. Finally, investigations for civil or disciplinary purposes suffer some of the same costs as criminal investigations, e.g., giving added publicity to the leak or confirming its accuracy, creating the impression of a cover-up, and, if the investigation is unsuccessful, demonstrating the impotence of the Government.

It has been suggested that the use of polygraphs could aid in such non-criminal investigations. The validity of polygraphs has always been a subject of some doubt, but the real utility of polygraphs is not in their ability to distinguish ultimately between truth and falsehood, but in their ability to intimidate persons into telling the truth--either initially because they believe a lie will be caught or after a lie, because the examiner reveals there has been an indication of a lie and asks the question again, giving the person the opportunity to change his response. In a non-criminal investigation a polygraph examination could only be

admin[illegible] been that refusal to undergo an examination results in no action against or inference of guilt toward the refuser.*/ Moreover, a polygraph can never be more than an adjunct to other investigative tools--the cost of using polygraphs would be excessive unless its use is restricted to situations in which the field of potential suspects had been narrowed to a rather small number.

It is current FBI practice to use polygraphs in security cases (including leaks) where it is deemed worthwhile, and therefore unless their use is intended to be substantially expanded, no change in policy is required.

It has also been suggested that further restricting access to classified information could help alleviate the problem of leaks. This could be effected in several ways, e.g., reducing the number of persons with security clearances, with the highest security clearances, or with codeword clearances; tightening the requirements for access to classified information even among persons who

---

*/ While consent to undergo a polygraph exam probably could be made a condition of employment in sensitive positions or to hold security clearances, such a requirement raises other questions, see infra.

have the proper clearance; increasing compartmentation by creation of new codewords.

Under E.O. 11652 before any person is allowed access to classified information he must have been determined to be trustworthy and his access to the information must be necessary for the performance of his duties. A security clearance is nothing more than the determination that a person is trustworthy. The fact that one has a security clearance should not mean that he has or should have access to any particular classified information. As a practical matter, however, the possession of the requisite security clearance is often considered sufficient grounds for giving someone classified information. Therefore, cutting the number of security clearances in the Government is likely to result in a certain diminution of unnecessary dissemination of classified information.

The question of a need-to-know as a requisite to access to classified information is often confused with the granting of a security clearance, and some departments and agencies do not grant specific clearances until a need-to-know has been established. The Subcommittee suggests that the review of E.O. 11652 should include consideration of changing the grounds for obtaining a security clearance, to require both a determination of trustworthiness and a need to work with classified information.

In addition, the Defense Department has had success with periodic reviews of the need for persons to have security clearances--in the sense that the reviews have resulted in substantial numbers of security clearances being removed as no longer necessary. The subcommittee recommends that the review of E.O. 11652 should consider a requirement of periodic reviews of the continuing necessity of existing security clearances.

It must be recognized, however, that elimination of unnecessary security clearances will likely bring only marginal results because those persons with unnecessary clearances normally do not in fact continue to have access.

And, further restricting access by a means other than reducing the number of unnecessary clearances would be of even less utility. Executive Order 11652 already restricts access to those who have a need-to-know, and access to certain compartmented information is on a "must know" basis. These standards should be enforced--and generally are--but it would seem that access to classified information within the Executive Branch cannot be further restricted without concurrently eliminating the newly established control and review mechanisms.

It is also questionable to what extent additional restrictions on access would be effective in stemming leaks. The persons from the Executive Branch who have been identified with publicized leaks of classified information (i.e., Ellsberg, Agee, Marchetti, Smith, Kahn) would have had justified access even under stricter standards. Moreover, with respect to untraced leaks apparently emanating from the Executive Branch, indications are that the persons responsible are small in number and rather well placed. In short, restrictions on access within acceptable limits are not likely to solve the problem.

While it might be useful to limit the number of Congressmen who are currently briefed on covert activities pursuant to the Hughes Amendment, 22 U.S.C. § 2422, and while the Executive Branch should encourage appropriate Congressional action, even if successful it is unlikely that such a limitation will meaningfully reduce the number of leaks.

Finally, the idea of creating more categories of compartmented information is criticized widely throughout the Intelligence Community, which is already questioning the cost-benefit relationship in the current compartmentations.

The use of polygraphs as a condition of access to certain information or to hold certain positions has been suggested. Polygraph tests now are required of applicants for employment at CIA and NSA, with follow-up polygraph examinations in the course of their careers. Consent to these examinations is a condition of both initial and continued employment. This procedure has never suffered any legal challenge or significant public disapprobation. While it cannot be demonstrated that these polygraph examinations have deterred leaks, it is reasonable to conclude that persons wishing continued employment would be deterred from leaking if subjected to periodic polygraph examinations.

Nevertheless, any meaningful expansion of polygraph examinations is likely to be met with criticism, and no feasible expansion could hope to cover all possible sources of leaks within the Executive Branch. Many of the personnel who fill the positions or have the access which would be covered by an expansion of the examinations are not career employees, and the threat of periodic examinations may not be meaningful to them because they expect to finish their Government service before they are examined again. Finally, certain agencies have expressed a loathing for polygraph

Why not a "retirement" polygraph as a matter of routine?

examin y that many individuals because of their position or prestige would feel insulted to be subjected to such an examination, and absent the most explicit Presidential direction, it would be impossible to enforce the requirement against such individuals.

It has also been suggested that the courts be used to enjoin the publication of classified information. There are severe problems, however, in obtaining such injunctions. Legally, there is some doubt whether with or without a specific statute authorizing such injunctions a court may ever enjoin the publication of information protected by the First Amendment. Nevertheless, under existing case law, it would appear that there are two situations in which an injunction against the publication of classified information might be obtained. The first is when the publication necessarily would result in substantial, direct, immediate, and irreparable damage to this Nation. See New York Times Co. v. United States, 403 U.S. 713 (1971) (Opinions of Brennan, Stewart, Burger, Harlan, and Blackmun). Obviously, it would take an extraordinary disclosure to meet this test, and this injunctive power is therefore of little benefit except in grave emergencies.

The other situation is where an injunction may be obtained to enforce a contract. This was the situation in United States v. Marchetti, 466 F.2d 1309 (4th Cir.), cert. denied, 409 U.S. 1063 (1972), where the United States obtained an injunction against the publication of certain sections of a book by a former CIA employee. The contract involved in that case was a secrecy agreement made by Marchetti in consideration for his employment with CIA. The success of the Government in the Marchetti case was quite limited in that substantial amounts of sensitive, classified information were allowed to be published. Moreover, injunctive relief premised upon secrecy agreements cannot hope to limit meaningfully the unauthorized disclosure of classified information, because it is the rare situation where the Government will have the prior knowledge of a disclosure necessary to obtain an injunction.

In E.O. 11905 the President required all employees of the Executive Branch and its contractors given access to information containing sources and methods of intelligence, as a condition of obtaining access, to undertake a Secrecy Agreement. See Section 7. Except for the CIA, however, which had already been using a Secrecy Agreement, other departments and agencies failed to carry out fully the mandate of the Section. Some agencies failed to require employees who already had access to execute agreements;

some agencies utilized Secrecy Oaths, rather than agreements, which are probably not judicially enforceable, see United States v. Marchetti, supra; some agencies did not require the Agreement of all employees because it would be demeaning or insulting to them; and some agencies are still trying to develop the language for a proper Agreement.

Even had the agencies fully complied with Section 7, there are certain inherent problems with Section 7 which render it fairly ineffectual even as to its limited objectives, i.e., to serve an additional educational and deterrent function and to serve as a basis for a civil injunction as in the Marchetti case. On the one hand, Section 7's Secrecy Agreement is limited to sources and methods; it does not cover classified information generally. In this respect the Agreement is underinclusive. On the other hand, the Agreement purports to protect all sources and methods, not just that which is classified, and it is doubtful whether a civil injunction can be obtained with respect to non-classified information, see United States v. Marchetti, supra. In this sense the Agreement is overinclusive.

For the above reasons, this subcommittee has recommended that Section 7 be deleted from E.O. 11905 and that the E.O. 11652 review should consider the

desirability of an improved Secrecy Agreement for possible inclusion in an amended E.O. 11652.

In any case, this subcommittee is of the view that a Secrecy Agreement will have only the most marginal, if any, effect on leaks of classified information. As noted above, the instances in which the Government will have prior knowledge of disclosure will be rare indeed and even in those cases courts will be loathe to enjoin broadly what the Government claims is classified. Moreover, the education and deterrent value of a Secrecy Agreement by itself is questionable; that is, it is doubtful that it would add anything to the secrecy oaths which have been required in the past, and, given the nature of the leaks in the past, it seems most unrealistic to think that a Secrecy Agreement would have deterred the leaks.

CONCLUSION:

Past experience indicates that there is an institutional unwillingness on the part of the Executive Branch to accept the costs and risks involved in criminal investigation and prosecution of leaks of classified information. On that basis, the enactment of new legislation to criminally punish the unauthorized disclosure of classified information would be a useless and politically costly exercise.

because the decision whether or not to investigate or prosecute has in the past been made or not made haphazardly without interagency consideration of concerns beyond the immediate leak, the subcommittee recommends that the SCC require all agencies to report to it any leak which has or is about to be widely disclosed. The SCC as a group should then consider the merits of investigating that leak civilly or criminally not only in light of the particular leak but also in terms of the likelihood of success in investigation and prosecution and the deterrent effect on other leaks.